In the Claims

1.   (**Currently Amended**)   A method comprising:

comparing first security level information and second security level information, wherein

~~said first security level information represents a first security level,~~

~~said second security level information represents a second security~~
~~level,~~

said first security level information is stored in a security label of a packet received at a network node of a network,

said first security level information represents a first security level,

said first security level is a security level of a source of said packet,

said second security level information is stored at said network node, ~~after~~
~~being~~

said second security level information is received from another network node of said network **as a result of said second security level information being registered in a context,**

said second security level information is configured to be updated by virtue of said second security level information being configured to be combined with third security level information,

said second security level information represents a second security level,

said second security level is a security level of a destination of said packet,

said network comprises a plurality of network nodes,

said network nodes comprise said network node and said another network node, and

said network nodes are configured to convey packets to one another via others of said network nodes; and

indicating processing to be performed on said packet based on said comparing, wherein

- 2 -

said processing comprises

    determining whether to forward said packet from said network

        node to one of said network nodes.

2.   (**Currently Amended**)   The method of claim 1, wherein said another network node is coupled to [[a]] <u>said</u> destination of said packet~~, and said destination is assigned said second security level~~.

3.   (Previously Presented)   The method of claim 1, wherein said first security level and said second security level implement one of a multi-level security paradigm and a multi-lateral security paradigm.

4.   (Previously Presented)   The method of claim 1, wherein said security label is one of an enumerated security label and a bitmap security label.

5.   (Previously Presented)   The method of claim 1, wherein said second security level is a security level of a port of said network node.

6.   (Original)   The method of claim 5, further comprising:

setting said security level of said port.

7.   (Original)   The method of claim 6, wherein said setting said security level of said port comprises:

    storing said second security level in a security label information field of an access

        control list entry.

8.   (Original)   The method of claim 6, wherein said setting said security level of said port comprises:

    storing said second security level in a label range information field of a

        forwarding table entry.

9.   (Previously Presented)   The method of claim 1, wherein said processing comprises:

      dropping said packet, if said comparing indicates that said first security level is less than said second security level.

10.   (Previously Presented)   The method of claim 1, wherein said processing comprises at least one of dropping said packet, redirecting said packet and rewriting said security label.

11.   (Previously Presented)   The method of claim 1, wherein said second security level information represents a plurality of security levels, and said security levels comprise said second security level.

12   (Original)   The method of claim 11, wherein said security levels are a range of security levels.

13   (Original)   The method of claim 12, wherein said processing comprises:

      dropping said packet, if said comparing indicates that said first security level is not within said range of security levels.

14.   (Original)   The method of claim 1, further comprising:

      storing said second security level information at said network node.

15.   (Original)   The method of claim 14, wherein said storing comprises:

      storing said second security level in a security label information field of an access control list entry.

16.   (Original)   The method of claim 14, wherein said storing comprises:

      storing said second security level in a label range information field of a forwarding table entry.

PATENT

17.   (**Currently Amended**)   The method of claim 14, wherein
said storing comprises[[:]]

~~communicating~~ **receiving** said second security level **information** from ~~a~~
~~first~~ **said another** network node ~~by registering~~ **, and**
said receiving occurs as a result of said second security level **being registered**
in [[a]] **said** context.

18.   (**Currently Amended**)   The method of claim 17, wherein said
~~registering comprises:~~ **second security level information is configured to be**
combined with said third security level information by virtue of said second security
level information being configured to be
~~updating said second security level information by~~ logically ~~OR'ing~~ **OR'd**
with said third security level information ~~with said second security level~~
~~information~~.

19.   (Original)   The method of claim 17, wherein
said context is a generic attribute registration protocol information propagation
context, and
said registering said second security level is accomplished by said first network
node issuing a join request.

20.   (Original)   The method of claim 14, wherein said storing comprises:
storing said second security level in a label range information field of forwarding
table.

21.   (Original)   The method of claim 14, wherein said storing comprises:
storing said second security level in a port of said network node.

22.   (Original)   The method of claim 21, wherein
said port is an egress port.

23.   (Previously Presented)   The method of claim 1, further comprising:

- 5 -

determining said first security level.

24. (Original) The method of claim 23, wherein said determining comprises:

determining if an ingress port is marked as an access port; and

setting a security level of said ingress port to said first security level, if said ingress port is marked as an access port.

25. (Original) The method of claim 24, further comprising:

setting said first security level information to said security level of said ingress port.

26. (Original) The method of claim 23, further comprising:

authenticating a user having said first security level, wherein

said determining is performed only if said user is authenticated.

27. (Previously Presented) The method of claim 1, further comprising:

performing said processing on said packet based on said comparing.

28. (Previously Presented) The method of claim 27, wherein said performing said processing comprises:

performing said forwarding of said packet, if said indicating indicates that said packet is allowed to be forwarded; and

dropping said packet, otherwise.

29. (Original) The method of claim 27, wherein said performing said processing comprises:

forwarding said packet to a firewall, if said indicating indicates that said packet should be forwarded to said firewall.

30. (Previously Presented) The method of claim 1, further comprising:

stripping network security information from said packet; and

adding subnetwork security information to said packet.

Application No.: 10/696,629

31.   (Original)   The method of claim 30, wherein
said network security information comprises said first security level information.

32.   (Original)   The method of claim 30, wherein
said subnetwork security information comprises said first security level
        information.

33.   (**Currently Amended**)   A computer system comprising:
a processor;
a **tangible** computer-readable storage medium coupled to said processor; and
computer instructions, encoded in said computer-readable storage medium,
        configured to cause said processor to:
        compare first security level information and second security level
                information, wherein
                        ~~said first security level information represents a first security~~
                                ~~level,~~
                        ~~said second security level information represents a second~~
                                ~~security level,~~
                        said first security level information is stored in a security label of a
                                packet received at a network node of a network,
                        **said first security level information represents a first security
                                level,**
                        **said first security level is a security level of a source of said
                                packet,**
                        said second security level information is stored at said network
                                node, ~~after being~~
                        said second security level information is received from another
                                network node of said network **as a result of said second
                                security level information being registered in a context**,
                        **said second security level information is configured to be
                                updated by virtue of said second security level
                                information being configured to be combined with third
                                security level information,**

- 7 -

said second security level information represents a second

security level,

said second security level is a security level of a destination of

said packet,

said network comprises a plurality of network nodes,

said network nodes comprise said network node and said another

network node, and

said network nodes are configured to convey packets to one

another via others of said network nodes; and

indicate processing to be performed on said packet based on said

comparing, wherein

said processing comprises

determining whether to forward said packet from said

network node to one of said network nodes.

34. (**Currently Amended**) The computer system of claim 33, wherein said another network node is coupled to [[a]] __said__ destination of said packet~~, and~~ ~~said destination is assigned said second security level~~.

35. (Previously Presented) The computer system of claim 33, wherein said computer instructions are further configured to cause said processor to:

set said security level of a port, wherein

said second security level is a security level of said port of said network

node.

36. (Previously Presented) The computer system of claim 35, wherein said computer instructions configured to cause said processor to set said security level of said port is further configured to cause said processor to:

store said second security level in a security label information field of an access

control list entry.

37. (Previously Presented) The computer system of claim 35, wherein said computer instructions configured to cause said processor to set said security level of said port is further configured to cause said processor to:

    store said second security level in a label range information field of a forwarding table entry.

38. (Cancelled)

39. (Previously Presented) The computer system of claim 33, wherein said computer instructions are further configured to cause said processor to:

    store said second security level information at said network node.

40. (Previously Presented) The computer system of claim 39, wherein said computer instructions configured to cause said processor to store is further configured to cause said processor to:

    store said second security level in a security label information field of an access control list entry.

41. (Previously Presented) The computer system of claim 39, wherein said computer instructions configured to cause said processor to store is further configured to cause said processor to:

    store said second security level in a label range information field of a forwarding table entry.

42. (Previously Presented) The computer system of claim 39, wherein said computer instructions configured to cause said processor to store is further configured to cause said processor to:

    communicate said second security level from a first network node by virtue of being configure to cause said processor to register said second security level in a context.

42.   (**Currently Amended**)   The computer system of claim 39, wherein said computer instructions configured to cause said processor to store is further configured to cause said processor to:

~~communicate~~ **receive** said second security level **information** from ~~a first~~ **said another** network node by virtue of being configure to cause said processor to register said second security level in **[[a]]** **said** context.

43.   (**Currently Amended**)   The computer system of claim 42, wherein said computer instructions configured to cause said processor to register **[[is]]** **are** further configured to cause said processor to:

~~update said second security level information by virtue of being configure to cause said processor to~~ logically OR **said** third security level information with said second security level information.

45.   (Previously Presented)   The computer system of claim 33, wherein said computer instructions are further configured to cause said processor to:

determine said first security level.

46.   (Previously Presented)   The computer system of claim 45, wherein said computer instructions are further configured to cause said processor to:

authenticate a user having said first security level, wherein

said computer instructions configured to cause said processor to determine said first security level causes said processor to determine said first security level only if said user is authenticated.

47.   (Previously Presented)   The computer system of claim 45, wherein said computer instructions configured to cause said processor to determine said first security level is further configured to cause said processor to:

determine if an ingress port is marked as an access port; and

set a security level of said ingress port to said first security level, if said ingress port is marked as an access port.

48.   (Previously Presented)   The computer system of claim 47, wherein said computer instructions are further configured to cause said processor to:

set said first security level information to said security level of said ingress port.

49.   (Previously Presented)   The computer system of claim 33, wherein said computer instructions are further configured to cause said processor to:

perform said processing on said packet based on a result generated by said
computer instructions configured to cause said processor to compare.

50.   (Previously Presented)   The computer system of claim 49, wherein said computer instructions configured to cause said processor to perform said processing on said packet is further configured to cause said processor to:

perform said forwarding of said packet, if said computer instructions configured
to cause said processor to indicate indicates that said packet is allowed to
be forwarded; and
drop said packet, otherwise.

51.   (Previously Presented)   The computer system of claim 33, wherein said computer instructions are further configured to cause said processor to:

strip network security information from said packet; and
add subnetwork security information to said packet.

52.   (**Currently Amended**)   A computer program product comprising:
a tangible computer-readable storage medium, wherein
        a plurality of sets of instructions are encoded in said tangible
                computer-readable medium, and
[[a]] **said** plurality of sets of instructions, ~~comprising~~ **comprise**
        a first set of instructions, executable on a computer system,
                configured to compare first security level information and
                second security level information, wherein
                ~~said first security level information represents a first~~
                ~~security level,~~

- 11 -

~~said second security level information represents a~~

~~second security level,~~

said first security level information is stored in a security
label of a packet received at a network node of a
network,

said first security level information represents a first

security level,

said first security level is a security level of a source of

said packet,

said second security level information is stored at said
network node, ~~after being~~

said second security level information is received from
another network node of said network **as a result of**

said second security level information being

registered in a context,

said second security level information is configured to

be updated by virtue of said second security level

information being configured to be combined

with third security level information,

said second security level information represents a

second security level,

said second security level is a security level of a

destination of said packet,

said network comprises a plurality of network nodes,

said network nodes comprise said network node and said
another network node, and

said network nodes are configured to convey packets to one
another via others of said network nodes, and

a second set of instructions, executable on said computer system,
configured to indicate processing to be performed on said
packet based on said comparing, wherein
said processing comprises

- 12 -

determining whether to forward said packet from
said network node to one of said network
nodes~~; and~~

~~a computer-readable storage medium, wherein said sets of instructions are~~
~~encoded in said computer-readable medium~~.

53. (**Currently Amended**) The computer program product of claim 52,
wherein
said another network node is coupled to a destination of said packet~~, and~~
~~said destination is assigned said second security level~~.

54. (Previously Presented) The computer program product of claim 52,
further comprising:
a third set of instructions, executable on said computer system, configured to set
said security level of a port, wherein
said second security level is a security level of said port of said network
node.

55. (Original) The computer program product of claim 54, wherein said
third set of instructions comprises:
a first subset of instructions, executable on said computer system, configured to
store said second security level in a security label information field of an
access control list entry.

56. (Original) The computer program product of claim 54, wherein said
third set of instructions comprises:
a first subset of instructions, executable on said computer system, configured to
store said second security level in a label range information field of a
forwarding table entry.

57. (Cancelled)

- 13 -

58.   (Original)   The computer program product of claim 52, further comprising:

 a third set of instructions, executable on said computer system, configured to store said second security level information at said network node.

59.   (Original)   The computer program product of claim 58, wherein said third set of instructions comprises:

 a first subset of instructions, executable on said computer system, configured to store said second security level in a security label information field of an access control list entry.

60.   (Original)   The computer program product of claim 58, wherein said third set of instructions comprises:

 a first subset of instructions, executable on said computer system, configured to store said second security level in a label range information field of a forwarding table entry.

61.   (**Currently Amended**)   The computer program product of claim 58, wherein said third set of instructions comprises:

 a first subset of instructions, executable on said computer system, configured to ~~communicate~~ **receive** said second security level from ~~a first~~ **said another** network node comprises a first sub-subset of instructions, executable on said computer system, configured to cause said processor to register said second security level in **[[a]]** **said** context.

62.   (**Currently Amended**)   The computer program product of claim 61, wherein said first sub-subset of instructions comprises:

 a first sub-sub-subset of instructions, executable on said computer system, configured to ~~update said second security level information comprises a first sub-sub-sub-subset of instructions, executable on said computer system configure to cause said processor to~~ logically OR **said** third security level information with said second security level information.

63.   (Original)   The computer program product of claim 62, wherein said context is a generic attribute registration protocol information propagation context, and

said first sub-subset of instructions is further configured to cause said first network node to issue a join request.

64.   (Previously Presented)   The computer program product of claim 52, further comprising:

a third set of instructions, executable on said computer system, configured to determine said first security level.

65.   (Original)   The computer program product of claim 64, further comprising:

a fourth set of instructions, executable on said computer system, configured to authenticate a user having said first security level, wherein

said third set of instructions is further configured to cause said processor to determine said first security level only if said user is authenticated.

66.   (Original)   The computer program product of claim 64, wherein said third set of instructions comprises:

a first subset of instructions, executable on said computer system, configured to determine if an ingress port is marked as an access port; and

a second subset of instructions, executable on said computer system, configured to set a security level of said ingress port to said first security level, if said ingress port is marked as an access port.

67.   (Original)   The computer program product of claim 66, further comprising:

a fifth set of instructions, executable on said computer system, configured to set said first security level information to said security level of said ingress port.

68.   (Previously Presented)   The computer program product of claim 52, further comprising:

a third set of instructions, executable on said computer system, configured to

perform said processing on said packet based on a result generated by said

first set of instructions.

69.   (Previously Presented)   The computer program product of claim 68, wherein said third set of instructions comprises:

a first subset of instructions, executable on said computer system, configured to

perform said forwarding of said packet, if said second set of instructions

indicates that said packet is allowed to be forwarded; and

a second subset of instructions, executable on said computer system, configured

to drop said packet, otherwise.

70.   (Previously Presented)   The computer program product of claim 52, further comprising:

a third set of instructions, executable on said computer system, configured to strip

network security information from said packet; and

a fourth set of instructions, executable on said computer system, configured to add

subnetwork security information to said packet.

71.-75. (**Cancelled**)

76.   (Cancelled)

77.-89. (**Cancelled**)

90.   (**Currently Amended**)   A network device comprising:
a network interface, wherein

said network interface is configured to receive a packet, and

said network device is configured to

store first security level information,

compare said first security level information and second security

level information, wherein

~~said first security level information represents a first~~

~~security level,~~

~~said second security level information represents a~~

~~second security level,~~

said first security level information is stored in a security

label of a packet received at a network node of a

network,

said first security level information represents a first

security level,

said first security level is a security level of a source of

said packet,

said second security level information is stored at said

network node, ~~after being~~

said second security level information is received from

another network node of said network **as a result of**

said second security level information being

registered in a context,

said second security level information is configured to

be updated by virtue of said second security level

information being configured to be combined

with third security level information,

said second security level information represents a

second security level,

said second security level is a security level of a

destination of said packet,

said network comprises a plurality of network nodes,

said network nodes comprise said network node and said

another network node, and

said network nodes are configured to convey packets to one

another via others of said network nodes, and

- 17 -

indicate processing to be performed on said packet based on said
comparing, wherein
said processing comprises
determining whether to forward said packet from
said network node to one of said network
nodes, and
perform said processing of said packet.

91.   (Original)   The network device of claim 90, wherein
said network interface comprises a port, and
 said port is configured to store said first security level information.

92.   (Original)   The network device of claim 91, wherein
said port is an egress port.

93.   (Original)   The network device of claim 91, wherein
said network device is further configured to set a security level of said port.

94.-95. (Cancelled)

96.   (Previously Presented)   The network device of claim 90, wherein
said network device is further configured to process said packet based on said
        comparing.

97.   (Previously Presented)   The network device of claim 90, wherein
said network device is further configured to strip network security information
        from said packet and add subnetwork security information to said packet.

98.   (Previously Presented)   The network device of claim 90, wherein
said first security level is a security level of a port of said network device.

99.   (Previously Presented)   The network device of claim 90, wherein
said second security level information represents a second security level, and
said first security level information represents a plurality of security levels.

100. (Original) The network device of claim 99, wherein said security levels are a range of security levels.

101. (Previously Presented) The network device of claim 90, wherein said network device is further configured to store said first security level information at said network device.

102. (Original) The network device of claim 101, wherein said network device is further configured to communicate said first security level from a second network device by registering said first security level in a context.

103. (Original) The network device of claim 102, wherein said context is a generic attribute registration protocol information propagation context, and said registering said first security level is accomplished by said second network device issuing a join request.

104. (**Currently Amended**) A network device comprising:
a content-addressable memory; and
an access control list, wherein
said content-addressable memory is configured to store said access control list,
said access control list comprises an access control list entry,
said access control list entry comprises a label information field,
said label information field is configured to store a security label, and
said network device is configured to
compare first security level information and second security level information, wherein
~~said first security level information represents a first security level,~~
~~said second security level information represents a second security level,~~

- 19 -

said first security level information is stored in a security label of a packet received at a network node of a network,

said first security level information represents a first security level,

said first security level is a security level of a source of said packet,

said second security level information is stored at said network node, ~~after being~~

said second security level information is received from another network node of said network **as a result of said second security level information being registered in a context**,

said second security level information is configured to be updated by virtue of said second security level information being configured to be combined with third security level information,

said second security level information represents a second security level,

said second security level is a security level of a destination of said packet,

said network comprises a plurality of network nodes,

said network nodes comprise said network node and said another network node, and

said network nodes are configured to convey packets to one another via others of said network nodes; and

indicate processing to be performed on said packet based on said comparing, wherein

said processing comprises

determining whether to forward said packet from said network node to one of said network nodes.

- 20 -

105.   (Original)   The network device of claim 104, wherein said security label implements a multi-level security paradigm.

106.   (Original)   The network device of claim 104, wherein said security label implements a multi-lateral security paradigm.

107.   (Original)   The network device of claim 104, wherein said access control list entry further comprises:

    a flow label field, wherein

        said flow label field allows said access control list entry to be identified as a security labeled access control list entry.

108.   (Original)   The network device of claim 107, wherein said access control list entry further comprises:

    a plurality of flow specification fields, wherein

        said flow specification fields comprise information identifying processing to be performed on at least one flow.

109.   (Original)   The network device of claim 104, wherein said security label is configured to be compared to a security label of a packet.

110.   (Original)   The network device of claim 109, wherein said access control list entry further comprises:

    a flow specification field, wherein

        said flow specification field comprise information identifying processing to be performed on said packet.

111.   (Original)   The network device of claim 110, wherein said access control list entry further comprises:

    a flow label field, wherein

        said flow label field allows said access control list entry to be identified as a security labeled access control list entry.

112.   (**Currently Amended**)   A network device comprising:

a forwarding table, wherein

> said forwarding table comprises a plurality of forwarding table entries,
>
> at least one forwarding table entry of said forwarding table entries
>> comprises a label range field, and
>
> said network device is configured to
>> compare first security level information and second security level
>>> information, wherein
>>>> ~~said first security level information represents a first security level,~~
>>>>
>>>> ~~said second security level information represents a second security level,~~
>>>>
>>>> said first security level information is stored in a security label of a packet received at a network node of a network,
>>>>
>>>> **said first security level information represents a first security level,**
>>>>
>>>> **said first security level is a security level of a source of said packet,**
>>>>
>>>> said second security level information is stored at said network node, ~~after being~~
>>>>
>>>> **said second security level information is** received from another network node of said network **as a result of said second security level information being registered in a context**,
>>>>
>>>> **said second security level information is configured to be updated by virtue of said second security level information being configured to be combined with third security level information,**
>>>>
>>>> **said second security level information represents a second security level,**
>>>>
>>>> **said second security level is a security level of a destination of said packet,**
>>>>
>>>> said network comprises a plurality of network nodes,

- 22 -

said network nodes comprise said network node and said

another network node, and

said network nodes are configured to convey packets to one

another via others of said network nodes; and

indicate processing to be performed on said packet based on said

comparing, wherein

said processing comprises

determining whether to forward said packet from

said network node to one of said network

nodes.

113. (Original)   The network device of claim 112, wherein said at least one
forwarding table entry further comprises:

a port identifier field, wherein

a port identifier stored in said port identifier field identifies a port.

114. (Original)   The network device of claim 113, wherein

a security label stored in said label range field is associated with said port.

115. (Original)   The network device of claim 113, wherein said at least one
forwarding table entry further comprises:

a media access control (MAC) address field; and

a virtual local area network (VLAN) identifier field, wherein

a combination of said MAC address field and said VLAN identifier field

are associated with said port identifier field and said label range

field.

116. (Previously Presented)   The network device of claim 115, wherein

said address field is configured to store a MAC address,

said VLAN identifier field is configured to store a VLAN identifier,

said VLAN identifier identifies a VLAN, and

a combination of said MAC address and said VLAN identifier identify said port

and said security label.

- 23 -

117.   (Original)   The network device of claim 114, wherein said at least one forwarding table entry further comprises:

      a media access control (MAC) address field configured to store a MAC address, wherein

         said MAC address is associated with a security label stored in said label range field.

118.   (Original)   The network device of claim 112, wherein said at least one forwarding table entry further comprises:

      a virtual local area network (VLAN) identifier field, wherein

         a VLAN identifier stored in said VLAN identifier field identifies a VLAN, and

      said VLAN is associated with a security label stored in said label range field.